Hardening Linux dans le LAN

Objectifs de cette séquence d'exercices :

- Expliquer
- Implémenter la sécurité centralisée sur une machine Linux dans le LAN

Console à utiliser :

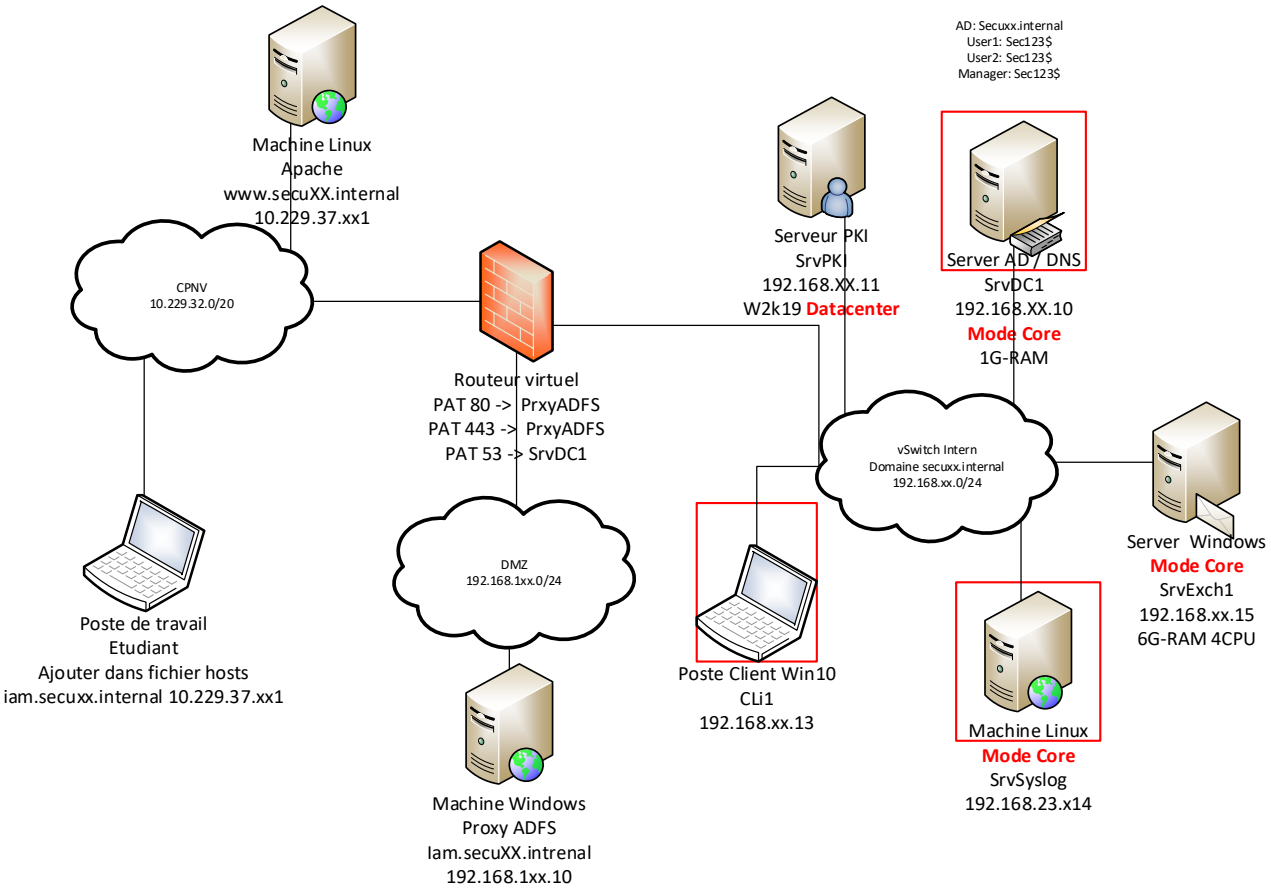
- Outil ssh : `putty.exe`

Documents/fichiers :

- https://www.server-world.info/en/note?os=Ubuntu_18.04&p=realmd
- https://wiki.debian.org/UnattendedUpgrades
- https://blog.ndk.name/linux-ssh-authentication-against-active-directory-without-joining-the-domain/
- https://pipo.blog/articles/20210803-ssh-allowed-commands

Schéma :

Machines nécessaires pour le module sont entourées en rouge



1 – Hardening machine Linux:

Cahier des charges :

13. En tant que responsable de la sécurité, je veux que mes serveurs linux soient à jour en permanence avec un minimum de downtime, dans le but de garantir un fonctionnement optimum du service.
14. En tant que responsable de la sécurité, je veux que l'authentification des techniciens se fassent à l'aide de compte de l'AD d'un groupe particulier ainsi qu'une clé RSA, dans le but de sécurisé l'accès à ces machines critiques et de faciliter de gestion des intervenants.
15. En tant que responsable de la sécurité, je veux qu'un utilisateur d'un groupe particulier puisse se connecter en ssh sur serveur et redémarrer que le service Apache, dans le but de déléguer les tâches répétitives à des personnes autres que les admins.
16. En tant que responsable de la sécurité, je veux que l'ensemble des logs (firewall et server web dans le WAN) des équipements réseaux puissent être centralisé, dans le but de surveiller l'infrastructure.

2 – Rapport de mise en service :

Rédiger un rapport de mise en services avec les points ci-dessous.

- Schéma à jour
- US13, extrait des modifications du(es) fichier(s) de conf
- US14, extrait des modifications du(es) fichier(s) de conf
- US15, extrait des modifications du(es) fichier(s) de conf
- Extrait des log du système centralisé